IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

Invicta Networks, Inc. Plaintiff, v. Trend Micro Inc. Defendant.	Civil Action No. 6:20-cv-766 The Honorable _____ **COMPLAINT FOR PATENT INFRINGEMENT** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT AND DEMAND FOR JURY TRIAL

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiff Invicta Networks, Inc. ("Invicta"), files this Original Complaint against Defendant Trend Micro Inc. ("Trend Micro") for infringement of U.S. Patent No. 7,010,698 ("'698 patent") and would respectfully show the Court as follows:

PARTIES

1. Plaintiff Invicta is a Delaware Corporation with its principal place of business located at 10217 Cedar Pond Drive, Vienna, VA 22182. The '698 patent is a seminal cybersecurity patent with a priority date of February 14, 2001 at the dawn of the Internet era (and which issued March 2, 2006), claiming systems and methods to protect computers and other devices from malicious code such as viruses, spyware, and other undesirable code.

2. On information and belief, Trend Micro Inc., was originally founded in the United States in 1988 and has its principal headquarters in Tokyo, Japan. Trend Micro has a United States headquarters, formed under the laws of California, with its principal place of business located at 225 East John Carpenter Freeway, Suite 1500, Irving, Texas 75062. Trend Micro also maintains an office within this judicial district, located at 11305 Alterra Parkway, Austin, Texas 78758.

Further, Trend Micro is registered to conduct business in Texas (Texas Taxpayer ID 77-0391563). The primary business of Trend Micro is the development and sale of security-related software for computers and the Internet (hereinafter referred to as "Deep Discovery Platform").

JURISDICTION AND VENUE

3. This is a civil action for patent infringement arising under the Patent Laws of the United States as set forth in 35 U.S.C. §§ 271, *et seq*.

4. This Court has federal subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a) and pendent jurisdiction over the other claims for relief asserted herein.

5. This Court has personal jurisdiction over Defendant pursuant to TEX. CIV. PRAC. & REM. CODE § 17.041 *et seq*. Personal jurisdiction exists over Defendant because Defendant has minimum contacts with this forum as a result of business regularly conducted within the State of Texas and within this judicial district, and, on information and belief, specifically as a result of, at least, committing the tort of patent infringement within Texas and this judicial district. Personal jurisdiction also exists because, on information and belief, Defendant, *inter alia*:

a. has substantial, continuous, and systematic business contacts in this judicial district:

b. owns, manages, and operates facilities within this judicial district (*e.g.*, the Austin office located at 11305 Alterra Parkway, Austin, Texas 78758);

c. actively advertises to residents within this judicial district to purchase infringing products and services;

d. actively advertises to residents of this judicial district to work for Trend Micro;

e. employs residents from this judicial district;

f. transacts business within the State of Texas;

g. continues to conduct such business in Texas through the continued operation within this judicial district; and

h. operates the Internet website, <https://www.trendmicro.com/en_us/business.html>, which is available to and accessed by customers and potential customers of the Defendant within this judicial district.

Accordingly, this Court's jurisdiction over the Defendant comports with the constitutional standards of fair play and substantial justice and arises directly from the Defendant's purposeful minimum contacts with the State of Texas.

6. This Court also has personal jurisdiction over the Defendant as Defendant has purposefully and voluntarily availed itself of the privilege of conducting business in the United States, the State of Texas, and specifically, this judicial district by continuously and systematically placing goods and services into the stream of commerce through an established distribution channel with the expectation that such good and services will be purchased by consumers within the United States, Texas, and this judicial district. Defendant, either directly and/or through intermediaries, uses, sells, offers to sell, distributes, advertises, and/or otherwise promotes the accused products in this judicial district. For example, Trend Micro reported sales of 37,351 million yen (~ $356MM) in North America for the period from January 1, 2019, to December 31, 2019. *Trend Micro Business Report (2019)*.[1] In Quarter 1 of 2020, Trend Micro reported sales of 8,877 million yen (~$85MM) in North America. *Trend Micro 2020 Q1 Financial Report Data.*

[1] Trend Micro continues to benefit from its infringing products and services, with 2019 yielding its highest annual revenue in the history of the company. *See* <https://www.businesswire.com/news/home/20200218005228/en/Trend-Micro-Reports-Highest-Annual-Revenue-Strongest>.

Additional information on U.S. sales can be found at <https://www.trendmicro.com/en_us/about/investor-relations/financial-reports-data.html>.

7. On information and belief, Trend Micro has authorized partners within Texas and specifically, this judicial district, (https://www.trendmicro.com/en_us/partners/find-a-partner.html), which are available to and accessed by customers and potential customers of the Defendant within this judicial district. On information and belief, Trend Micro products and services are sold to and by these third-party partners, including, *inter alia*:

a. ClearDATA, a managed service provider, located at 835 West Sixth Street, 12th Floor, Austin, Texas 78703. *See* <https://www.cleardata.com/> for more information.

b. Sirius Computer Solutions, Inc., a reseller, with locations at 10100 Reunion Place, Ste. 500, San Antonio, TX 78216 (corporate headquarters) and 7501 N. Capital of Texas Hwy, Bldg. A, Ste. 110, Austin, Texas 78731. *See* <https://www.siriuscom.com/> for more information.

c. Accudata Systems, Inc., a reseller, with full-time consultants and account management located in Austin and San Antonio. *See* <https://accudatasystems.com/> for more information.

d. Access Communications Group, LLC., a reseller, located at 2017 Texas Ave., El Paso, TX 79901. *See* <https://www.acglp.com/> for more information.

e. Alcon Data-Tel Solutions LLC, a managed service provider, located at 5808 Balcones Dr., Ste. 104, Austin, TX 78731. *See* <https://alcondts.com/> for more information.

f. Austin Computing Solutions, a reseller, located at 2120 W. Braker Ln., Ste. G., Austin, TX 78758. *See* <https://www.austincomputing.com/> for more information.

g. BFG Cyber Security Solutions, a reseller, located at 1 Chisholm Trail Rd., Round Rock, TX 78781. *See* <https://bfg-css.com/> for more information.

h. Bridgehead Networks, a reseller, located at 2810 N. Flores, St., San Antonio, TX 78212. See <http://www.bridgeheadnetworks.com/> for more information.

i. Centex Information Technologies, a reseller, with locations at 7600 Chevy Chase Dr. #300, Austin, TX 78752 and 501 N. 4th St., Killeen, TX 76541. See <https://www.centextech.com/> for more information.

As noted, these are only a small sample of Trend Micro Partners located within this judicial district. Including the above, and on information and belief, Trend Micro is partnered with at least 44 businesses with locations within this judicial district.

8. On information and belief, Trend Micro has Alliance Partnerships with at least 63 companies. <https://www.trendmicro.com/en_us/partners/explore-alliance-partners.html>. Many of these Alliance Partners have locations within this judicial district, including, *inter alia*: BlackBerry, Box, Cisco Systems, Dell, Dropbox, Google, Hewlett Packard Enterprise, Microsoft, etc.

9. Venue is proper in this Court under 28 U.S.C. §§ 1391(b), (c), (d) and 28 U.S.C. § 1400(b) based on the information and belief that the Defendant has committed or induced acts of infringement, and/or advertise, market, sell, and/or offer to sell products, including infringing products, in this judicial district, as discussed above in ¶¶ 2 and 5-8, which are incorporated by reference herein. On information and belief, and as stated above, Trend Micro has significant ties

to, and presence in, the State of Texas and the Western District of Texas, making venue in this judicial district both proper and convenient for this action.

10. By virtue of filing this complaint, Plaintiff voluntarily consents to this Court's jurisdiction and venue.

THE PATENT-IN-SUIT

11. On March 7, 2006, United States Patent No. 7,010,698 ("the '698 patent"), entitled "Systems and Methods for Creating a Code Inspection System" was duly and legally issued by the United States Patent and Trademark Office ("USPTO") to Victor I. Sheymov, with Invicta Networks, Inc. ("Invicta") as assignee. A copy of the '698 patent is attached hereto as **Exhibit A**.

12. Plaintiff Invicta Networks, Inc., is the owner of the entire right, title, and interest in and to the '698 patent, with the right to sue in its own name.

13. The '698 patent is presumed valid under 35 U.S.C. § 282.

THE PATENTED CODE INSPECTION SYSTEM TECHNOLOGY

14. Anyone who owns a smartphone, a computer, or accesses the Internet in any way is, or should be, aware of malware – software intentionally designed to disrupt, damage, or gain unauthorized access to a computer, server, smartphone, computer network, application, or any of the many appliances connected to the Internet, such as home security systems, cameras, or thermostats. Malware takes many forms, including, *inter alia*, computer viruses, worms, Trojan horses, ransomware, and spyware to name a few. The '698 patent is a seminal patent claiming systems and methods to protect computers and other devices from such malware or malicious code. The '698 patent claims priority to February 14, 2001 (at the dawn of the Internet era) and is directed to a code inspection system including a dynamic decoy system. In today's computer vernacular, such a code inspection system / dynamic decoy system may be referred to as a malware detector

or a "sandbox." One of skill in the art will understand that a "sandbox" creates a separate, secure test environment, isolated from the main network or host system, in which to execute or detonate a suspicious file or web address attached to an email or a webpage, without risking harm to the host system. If the file or web address displays malicious behavior, it is deleted before being passed to the protected host system. If the file or web address displays normal behavior, it is safely passed to the protected host system.

15. The '698 patent overcomes shortcomings in the prior art, which could only detect previously known malicious code contained in a "library" of known code (col. 1, lines 59-67), and was ineffective and inefficient in creating and maintaining multiple "test chambers" (decoy systems) due to the many different variations of code, malware, and operating systems (col. 2, lines 23-42). The '698 patent addresses the need to detect and protect the host system from both known and unknown malware, by using a test chamber (a dynamic decoy system) that can be updated to mirror the current protected system or host computer (col. 3, lines 9-44 and col. 4, lines 24-35), with the test chamber simulating the protected system, including for example, the protected CPU, system memory, and all devices. By updating and closely replicating the host or protected system, the dynamic decoy system provides users with the best evidence of how a suspected file or malicious code would behave on the host system, without risking access or harm to the host system. Such dynamic decoy updating systems, methods, and aspects were not well-understood, routine, or conventional at the time of the invention.

16. The '698 patent is well-known in the cybersecurity industry. It has been cited in at least 80 patents and patent applications, including patents and patent applications filed by industry leaders, such as AT&T Corp., the International Business Machine Corp., and Microsoft Corp.

17. Claim 1 of the '698 patent is representative of claims 7, 8, and 9, and claims, for example, a code inspection system comprising a code inspection management module, a dynamic decoy system, an actuator module, and one or more sensor modules – all of which cooperate with a protected system, while insulating the protected system from malicious code. In one embodiment, the code inspection management module monitors the protected system, while the dynamic decoy system is updated to parallel or emulate relevant portions of the protected system. In another embodiment, the sensor modules enable the decoy system to analyze actions and results of one or more portions of the code in response to stimuli from the actuator module.

18. Claim 10 (and 19) of the '698 patent is representative of claims 14 (and 23), 15 (and 24), 16 (and 25), and 18 (and 27), and claims, for example, information storage media and a method for creating and maintaining a dynamic decoy system based on a protected system. The claims comprise a dynamic decoy system, code that is received with the dynamic decoy system, and sensors monitoring such code within the dynamic decoy system. In one embodiment, the dynamic decoy system parallels or emulates potions of a protected system, and can be updated based on changes made to the protected system. In another embodiment, code is then introduced to the decoy system to simulate the operating conditions of the protected system and monitor actions and results.

TREND MICRO's INFRINGING DEEP DISCOVERY PLATFORM

19. On information and belief, Defendant provides data security, web security, email security, mobile security, data loss prevention software, insider threat protection, cloud security, network security, and cross domain solutions. In particular, Trend Micro's Deep Discovery Platform of products and services (*e.g.*, Deep Discovery Analyzer; Deep Discovery Inspector; Deep Discovery Web Inspector; Deep Discovery Email Inspector; etc.) provide -- as claimed in

the '698 patent – an isolation and code inspection environment that simulates a host system, including the CPU, system memory, and all devices, thereby infringing the '698 patent. For example, the Deep Discovery Analyzer (*e.g.,* code inspection system) provides secure, isolated operating system environments (*e.g.,* dynamic decoy systems) that are updated to simulate or mirror a host system (*e.g.,* protected system). Defendant's Deep Discovery Analyzer interacts (*e.g.,* actuator modules) with the malware and observes (*e.g.,* sensor modules) every action and result. The Deep Discovery Analyzer product integrates with Trend Micro's firewall, web security, email security, and cloud access security products, among others. On information and belief, the Deep Discovery Analyzer integrates with the following Trend Micro products, *inter alia*:

Sandbox Analysis – Products that can send samples to the Deep Discovery Analyzer for sandbox analysis, include at least the following:

a. Apex One as a Service;

b. Apex One 2019;

c. Deep Discovery Email Inspector 2.5 or later;

d. Deep Discovery Inspector 3.7 or later;

e. Deep Discovery Web Inspector 2.5;

f. ScanMail for Microsoft Exchange 11.0 or later;

g. ScanMail for IBM Domino 5.6 SP1 Patch 1 HF466 or later;

h. InterScan Messaging Security Virtual Appliance 8.3 SP2 or later;

i. InterScan Messaging Security Suite for Windows 7.5 or later;

j. InterScan Web Security Virtual Appliance 6.0 or later;

k. InterScan Web Security Suite 6.5;

l. InterScan Messaging Security Suite for Linux 9.1;

m. Deep Security 10.0 or later;

n. Deep Edge 2.5 SP2 or later;

o. OfficeScan XG or later;

p. Trend Micro Endpoint Sensor 1.6 or later;

q. Trend Micro TippingPoint Security Management System 5.0 or later; and

r. Trend Micro Web Security 3.1.

Suspicious Object List – Products that retrieve the suspicious object list from the Deep Discovery Analyzer include at least the following:

a. Apex Central 8.0 Patch 1,

b. Deep Discovery Email Inspector 2.5 or later;

c. Deep Discovery Inspector 3.7 or later;

d. Deep Discovery Web Inspector 2.5;

e. Standalone Smart Protection Server with the latest patch 2.6 or later;

f. OfficeScan Integrated Smart Protection Server 10.6 SP2 Patch 1 to OfficeScan Integrated Smart Protection Server 11 SP1;

g. InterScan Web Security Virtual Appliance 6.0 or later;

h. InterScan Web Security Suite 6.5;

i. Control Manager 7.0 Patch 1 (with the latest hotfix installed); and

j. Trend Micro Web Security 3.1.

Exceptions – Products that send exceptions to the Deep Discovery Analyzer include at least the following:

a. Apex Central 8.0 Patch 1; and

b. Control Manager 7.0 Patch 1 (with the latest hotfix installed).

See, Trend Micro Deep Discovery Analyzer Administrator's Guide 6.9, https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf, at 2-6 to 2-9.

20. On further information and belief, Defendant's Virtual Analyzer integrates and interacts with Defendant's Deep Discovery Platform of products. Trend Micro describes the Virtual Analyzer as:

> Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration. *See* https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf (Chapter 4).

21. For the purposes of this Complaint, the term "Trend Micro Deep Discovery Platform" encompasses all such code inspection and isolation functionalities and any related or integrated Trend Micro security technologies, software, products, and services (*e.g.*, Deep Discovery Analyzer; Deep Discovery Inspector; Deep Discovery Director; Virtual Analyzer; etc.).

COUNT I
INFRINGEMENT OF THE '698 PATENT

22. Plaintiff Invicta repeats and realleges the above paragraphs, which are incorporated by reference as if fully restated herein.

23. Plaintiff Invicta is the owner by assignment of all right, title, and interest in and to the '698 patent, including all right to recover for any and all infringement thereof.

24. Plaintiff Invicta has not licensed or otherwise authorized Defendant to practice under the '698 patent.

25. The '698 patent is presumed valid under 35 U.S.C. § 282.

26. The '698 patent relates to, among other things, systems and methods for creating a code inspection system including a dynamic decoy system that is updated to mirror a protected host system.

27. On information and belief, Defendant has infringed the '698 patent by making, having made, using, importing, providing, supplying, distributing, testing, selling, or offering for sale a code inspection system, as described and claimed in the '698 patent, which simulates a host system, including for example, the protected CPU, system memory, and all devices. For example, Trend Micro's Deep Discovery Platform of products including the Deep Discovery Analyzer, which is integrated into many Trend Micro products, infringe the '698 patent.

28. On information and belief, Defendant continues to engage in infringing acts, as described above, with knowledge of the '698 patent by the filing of this Complaint, and with the actual intent to cause the acts which it knew or should have known would directly infringe, individually or jointly, and induce actual infringement.

Defendant's Direct Infringement of the '698 Patent

29. On information and belief, in violation of 35 U.S.C. § 271(a), Defendant has directly infringed, continues to directly infringe, and will continue to directly infringe, individually or jointly, absent this Court's intervention, one or more claims of the '698 patent, including for example (but not limited to) at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the '698 patent, either literally or under the doctrine of equivalents, by making, distributing, using, testing, selling, and/or offering to sell within the United States, or importing into the United States, without license or authority, Defendant's suite of infringing computer-security related software products, including, but not limited to, malware detection software that simulates a host system for isolation and inspection. For example, Trend Micro's Deep Discovery Platform and such related products as described in ¶¶ 19-20.

Direct Infringement Allegations

30. ***Direct Infringement Claim Charts:*** Exhibits 1 and 2 illustrate how Trend Micro's Deep Discovery Platform and related products and services perform the claimed systems, methods, and information storage media. Such infringement of the '698 patent by Trend Micro's Deep Discovery Platform is exemplified in Exhibits 1 and 2 focusing on Trend Micro's Deep Discovery Analyzer, Inspector, Director, and Virtual Analyzer. However, a person of ordinary skill in the art would readily recognize the broader implications of these representative materials.

31. On information and belief, and as demonstrated in **Exhibit 1**, Defendant Trend Micro performs each limitation of claim 1 of the '698 patent:

> "1. A code inspection system comprising:
> a code inspection management module that monitors and communicates with a protected system;
> a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;
> an actuator module; and
> one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,
> wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system."

32. On information and belief, and as demonstrated in **Exhibit 1** (claim 1 is representative), Defendant Trend Micro performs each limitation of claim 7 of the '698 patent:

> "7. A code inspection system comprising:
> a code inspection management module that monitors and communicates with a protected system;
> a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;
> an actuator module; and
> one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,
> wherein at least a portion of the protected system is capable of being recovered from the dynamic decoy system.

33. On information and belief, and as demonstrated in **Exhibit 1** (claim 1 is representative), Defendant Trend Micro performs each limitation of claim 8 of the '698 patent:

> "8. A code inspection system comprising:
> a code inspection management module that monitors and communicates with a protected system;
> a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;
> an actuator module; and
> one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,
> wherein the code inspection system is an interface between the protected system and one or more unprotected systems."

34. On information and belief, and as demonstrated in **Exhibit 1** (claim 1 is representative), Defendant Trend Micro performs each limitation of claim 9 of the '698 patent:

> "9. A code inspection system comprising:
> a code inspection management module that monitors and communicates with a protected system;
> a dynamic decoy system that, in cooperation with the code inspection management module, is updated to substantially parallel relevant portions of the protected system;
> an actuator module; and
> one or more sensor modules, wherein the dynamic decoy system is capable of analyzing at least one of actions and results of one or more portions of code in response to stimuli from the actuator module,
> wherein the code inspection management module monitors the protected system and updates the dynamic decoy system based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices."

35. On information and belief, and as demonstrated in **Exhibit 2**, Defendant Trend Micro performs each limitation of claim 10 of the '698 patent:

> "10. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:
> creating a dynamic decoy system that substantially parallels relevant portions of a protected system;
> updating the dynamic decoy system based on changes to the protected system;
> receiving one or more portions of code;
> introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system; and

monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,

wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system."

36. On information and belief, and as demonstrated in **Exhibit 2** (claim 10 is representative), Defendant Trend Micro performs each limitation of claim 14 of the '698 patent:

"14. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system;

and monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,

wherein the dynamic decoy system is an interface between the protected system and one or more unprotected systems."

37. On information and belief, and as demonstrated in **Exhibit 2** (claim 10 is representative), Defendant Trend Micro performs each limitation of claim 15 of the '698 patent:

"15. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:

creating a dynamic decoy system that substantially parallels relevant portions of a protected system;

updating the dynamic decoy system based on changes to the protected system;

receiving one or more portions of code;

introducing the one or more portions of code to the dynamic decoy system;

simulating operating conditions of the protected system in the dynamic decoy system;

monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code; and

installing one or more sensors in the dynamic decoy system that detect one or more of unauthorized access attempts, unauthorized command execution attempts and unauthorized modifications to one or more portions of the dynamic decoy machine."

38. On information and belief, and as demonstrated in **Exhibit 2** (claim 10 is representative), Defendant Trend Micro performs each limitation of claim 16 of the '698 patent:

> "16. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:
> creating a dynamic decoy system that substantially parallels relevant portions of a protected system;
> updating the dynamic decoy system based on changes to the protected system;
> receiving one or more portions of code;
> introducing the one or more portions of code to the dynamic decoy system;
> simulating operating conditions of the protected system in the dynamic decoy system;
> monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code; and
> installing an actuator in the dynamic decoy system."

39. On information and belief, and as demonstrated in **Exhibit 2** (claim 10 is representative), Defendant Trend Micro performs each limitation of claim 18 of the '698 patent:

> "18. A method of creating and maintaining a dynamic decoy system based on a protected system comprising:
> creating a dynamic decoy system that substantially parallels relevant portions of a protected system;
> updating the dynamic decoy system based on changes to the protected system;
> receiving one or more portions of code;
> introducing the one or more portions of code to the dynamic decoy system;
> simulating operating conditions of the protected system in the dynamic decoy system; and
> monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,
> wherein updating the dynamic decoy system is based on at least one of installed software, installed hardware, operating system upgrades, software upgrades, hardware upgrades, software deletions, hardware deletions and input/output devices."

40. The method claims and information storage media claims have similar claim language, as shown in the following independent claim pairs: 10 (19), 14 (23), 15 (24), 16 (25) and 18 (27). Plaintiff relies on **Exhibit 2** (of which claim 10 is representative), and ¶¶ 35-39 *supra*, on information and belief, as providing sufficient notice to Defendant Trend Micro that it performs each limitation of the information storage media claims of the '698 patent.

41. On information and belief, Defendant Trend Micro's accused products and services – the Deep Discovery Platform (*e.g.*, Deep Discovery Analyzer) – embody each limitation of the dependent claims 2-6, 11-13, 17, 20-22, and 26 of the '698 patent. Reasonable discovery will confirm this interpretation. *See* **Exhibit 1** (claim 1 is representative) and **Exhibit 2** (claim 10 is representative).

Defendant's Direct Infringement of the Method Claims

42. Defendant performs the methods recited in claims 10-18 of the '698 patent. Infringement of a method claim requires performing every step of the claimed method. Defendant performs every step of the methods recited in claims 10-18. As set forth above, Defendant performs, for example, the method recited in claim 10, *i.e.*, "10. A method of creating and maintaining a dynamic decoy system based on a protected system comprising: creating a dynamic decoy system that substantially parallels relevant portions of a protected system; updating the dynamic decoy system based on changes to the protected system; receiving one or more portions of code; introducing the one or more portions of code to the dynamic decoy system; simulating operating conditions of the protected system in the dynamic decoy system; and monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code, wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system."

43. Even if one or more steps recited in method claims 10-13, 14, 15, 16-17, and 18 are performed through technologies not in the physical possession of the Defendant (*e.g.*, in the possession of Trend Micro's partners, resellers, end-users, etc.), the claimed method are specifically performed by Trend Micro's products and services, such as the Deep Discovery

Analyzer. Defendant directly infringes as its products and service – Deep Discovery Platform (*e.g.*, Deep Discovery Analyzer) – dictate the performance of the claimed steps, such as the "creating," "updating," "receiving," "simulating," and "monitoring" steps recited in claim 10 of the '698 patent. Defendant's products and services are designed and built by Defendant to perform the claimed steps automatically. On information and belief, only Defendant can modify the functionality relating to these activities; no one else can modify such functionality. Defendant therefore performs all of the claimed steps and directly infringe the asserted method claims of the '698 patent, as demonstrated in **Exhibit 2**.

44. ***Additionally or alternatively***, to the extent third parties or end-users perform one or more steps of the methods recited in claims 10-18 of the '698 patent, any such action by third parties and/or end-users is attributable to Defendant, such that Defendant is liable for directly infringing such claims in a multiple actor or joint infringement situation, because Defendant directs or controls the other actor(s). In this regard, Defendant conditions participation in activities, as well as the receipt of benefits, upon performance of any such step by any such third party or end-user. Defendant exercises control over the methods performed by its products and services – for example Trend Micro's Deep Discovery Platform (*e.g.*, Deep Discovery Analyzer) – and benefit from others' use, including without limitation creating and receiving ongoing revenue streams from the accused products and related goods, and improvement/enhancement of its products and services. End-users and third parties receive a benefit from fiscal gains (*e.g.,* third-party resellers; partners increasing the value of their own products and service through use of Trend Micro's products and services) and enhanced cybersecurity (*e.g.*, end-users and third parties are protected from malware or malicious code). Such security forms the basis of entire businesses, such as those listed above as Trend Micro partners. Defendant also establishes the manner and timing of that

performance by the third-party or end-user, as dictated by the claimed method steps. All third-party and end-user involvement, if any, is incidental, ancillary, or contractual.

45. Thus, to the extent that any step of the asserted method claims is performed by someone other than Defendant (*e.g.*, an end-user or third party), Defendant nonetheless directly infringes the '698 patent at least by one or more of: (1) providing products and services, for example the Deep Discovery Platform (*e.g.*, Deep Discovery Analyzer), built and designed to perform methods covered by the asserted method claims; (2) dictating via software and associated directions and instructions (*e.g.*, to end-users) the use of the accused products such that, when used as built and designed by Defendant, such products perform the claimed methods; (3) having the ability to terminate others' access to and use of the accused products and related goods and services if the accused products are not used in accordance with Defendant's required terms; (4) marketing and advertising the accused products, and otherwise instructing and directing the use of the accused products in ways covered by the asserted method claims; and (5) updating and providing ongoing support and maintenance for the accused products.

Defendant's Direct Infringement of the System and Information Storage Media Claims

46. Defendant makes, uses, sells, offers to sell, and/or imports the code inspection systems recited in claims 1-9, and the information storage medias recited in claims 19-27. Such claims are infringed when an accused system or media, having every element of the claimed system or media, is made, used, sold, offered for sale, or imported within the United States. Defendant makes, uses, sells, offers to sell, and/or imports the accused products (or cause such acts to be performed on its behalf), which possess every element recited in claims 1-9 and 19-27, as set forth in more detail above and demonstrated in **Exhibit 1** and **Exhibit 2** attached. Defendant therefore directly infringes the system and media claims of the '698 patent.

47. ***Additionally or alternatively,*** regarding any "use" of the accused systems "by customers," which is a subset of the direct infringement of system claims, Defendant directly infringes in such situations, as Defendant puts the accused products and services into service and, at the same time, controls the system as a whole and obtains benefit from it. Defendant provides all components in the system and controls all aspects of its functionality. Although third parties (*e.g.*, Trend Micro partners, etc.) and end-users (*e.g.*, customers) may have physical control over certain aspects of the accused systems, Defendant retains control over how the accused system operates (*e.g.*, by having built and designed its products and services, for example the Deep Discovery Analyzer, to automatically inspect and analyze potentially malicious code (and similar data) in a particular, non-modifiable manner). The nature and extent of Defendant's control over the system, and the benefits realized from each element of the claims, was discussed above in connection with the asserted method claims. Such discussion is incorporated herein by reference. Defendant collects valuable data through its control of this system, which in turn is used to optimize, improve, and enhance Trend Micro's systems, products, services, etc. as a whole – again benefitting Defendant.

48. ***In the alternative,*** if the end-user or third-party is deemed to put the invention into service and controls the system as a whole, the end-user and third-party benefit from each element of the claims because Defendant's products and services, for example the Deep Discovery Platform (*e.g.*, Deep Discovery Analyzer), are designed and built by Defendant to perform the claimed steps automatically. End-users receive a benefit from putting the invention into service, thereby protecting their personal or business computer systems, networks, etc., from possible cyberattacks and malware. Third parties (*e.g.*, Trend Micro partners, etc.) receive a benefit from putting the invention into service by improving their own products and services, which improves their own

profits. Further, and on information and belief, third-party partners share a fiscally/contractually beneficial relationship with Trend Micro. In both cases, Trend Micro would be liable as an inducing infringer as described below.

Induced Infringement

49. Defendant has induced and will continue to induce others' infringement of claims 1-27 of the '698 patent, in violation of 35 U.S.C. § 271(b). As of the date of this filing, Defendant has actively encouraged infringement of the '698 patent, knowing that the acts it induced constituted infringement of the '698 patent, and its encouraging acts actually resulted in direct patent infringement by others.

50. On information and belief, Defendant has and continues to promote, advertise, and support end-users (*e.g.,* customers) and third parties (*e.g.*, Trend Micro partners) of its Deep Discovery Platform, with actions to include, but not limited to the following:

(i) Defendant's advertising Trend Micro's Deep Discovery Platform of product, for example its Deep Discovery Analyzer, on its website <https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html>;

(ii) Defendant's providing data sheets, blog posts, and webinars to potential customers from its website <https://www.trendmicro.com/en_us/about/webinars-customer.html>, <https://blog.trendmicro.com/highlighting-the-value-of-deep-security-and-deep-discovery-at-the-university-of-new-brunswick/>, <www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/inspector.html?modal=s3b-prd-img-datasheet-6337c1>;

(iii) Defendant's providing technical support from its website <https://success.trendmicro.com/technical-support?_ga=2.177451809.581513791.1595263670-1666404359.1594740537>, and also providing detailed technical documentation regarding installing, operating, and troubleshooting the software <https://docs.trendmicro.com/all/ent/ddi/v3.5/en-us/ddi_3.5_ag.pdf>; and

(iv) Defendant's providing an extensive partner/reseller program for selling and supporting the software <https://www.trendmicro.com/en_us/partners/find-a-partner.html>.

Defendant controls the distribution and implementation of its Deep Discovery Platform of products. On information and belief, Defendant continues to engage in these acts with knowledge of the '698 patent by the filing of this Complaint, and with the actual intent to cause the acts which it knew or should have known would induce actual infringement.

Damage to Invicta Networks Inc.

51. Defendant Trend Micro has infringed the '698 patent by making, having made, using, importing, providing, supplying, distributing, testing, selling, or offering for sale code inspection systems utilizing methods for creating and maintaining a dynamic decoy system, and related information storage media.

52. On information and belief, Defendant's actions have and continue to constitute active inducing infringement of at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the '698 patent in violation of 35 U.S.C. §271(b).

53. As a result of Defendant's infringement of at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the '698 patent, Plaintiff Invicta has suffered monetary damages in an amount yet to be determined, not less than a

reasonable royalty, and will continue to suffer damages in the future unless Defendant's infringing activities are enjoined by this Court.

54. Defendant's wrongful acts have damaged and will continue to damage Plaintiff Invicta irreparably, and Plaintiff has no adequate remedy at law for those wrongs and injuries. In addition to its actual damages, Plaintiff Invicta is entitled to a permanent injunction restraining and enjoining Defendant and its agents, servants, and employees, and all person acting thereunder, in concert with, or on its behalf, from infringing at least code inspection system claims 1-9, method claims 10-18, and information storage media claims 19-27 of the '698 patent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Invicta respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff Invicta that Defendant has been and is infringing at least claims 1-27 of the '698 patent pursuant to 35 U.S.C. §§ 271(a) and/or 271(b);

B. A permanent injunction enjoining Defendant and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert or privity with any of them from infringing, or inducing the infringement of, at least claims 1-27 of the '698 patent;

C. A judgment awarding Plaintiff Invicta all damages adequate to compensate it for Defendant's infringement of the '698 patent under 35 U.S.C. § 284, and in no event less than a reasonable royalty for Defendant's acts of infringement, including all pre-judgement and post-judgment interest at the maximum rate permitted by law, and also any past damages permitted under 35 U.S.C. § 286, as a result of Defendant's infringement of at least at least claims 1-27 of the '698 patent;

D. An assessment of costs, including reasonable attorney fees pursuant to 35 U.S.C. § 285, and prejudgment interest against Defendant; and

E. Any other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Pursuant to FED. R. CIV. P. 38, Plaintiff Invicta hereby demands a trial by jury on all issues so triable.

Dated: August 24, 2020

Respectfully submitted,

By: /s/ Thomas M. Dunlap
Thomas M. Dunlap (Admitted W.D. Tex./VA Bar No. 44016)
David Ludwig (Admitted W.D. Tex./VA Bar No. 73157)
Dunlap Bennett & Ludwig PLLC
8300 Boone Blvd., Suite 550
Vienna, Virginia 22182
(703) 777-7319 (t)
(703) 777-3656 (f)
tdunlap@dbllawyers.com
dludwig@dbllawyers.com
ecf@dbllawyers.com

Attorneys for Invicta Networks, Inc.